

Computer Algebra

Sebastian Iwanowski
FH Wedel

6. Polynomarithmetik
Teil 2: Division und Einfache Faktorisierung

Referenzen zum Nacharbeiten:

Köpf 6.4-6.9

von zur Gathen, Gerhard, Kapitel 3, 5 (zur Vertiefung, u.a. für die Laufzeitabschätzung)

Seminararbeit 6 (Stefan Hasenbanck)

Computer Algebra 6

Division von Polynomen p und q

Definition:

Ein Ring R heißt Euklidischer Ring, wenn es für jedes Element $p \in R$ eine Gradfunktion $\deg: R \rightarrow \mathbb{N}$ gibt mit:

- i) $\forall p, q \in R \exists s, r \in R: p = s \cdot q + r$ und $\deg(r) < \deg(q)$
- ii) $\deg(0) = 0$ und $\forall p, q \in R \setminus \{0\}: \deg(p \cdot q) \geq \deg(p)$

Beispiele:

- Jeder Körper ist ein Euklidischer Ring.
- \mathbb{Z} ist ein Euklidischer Ring.
- Die Menge $K[x]$ der Polynome über K bildet für jeden Körper K einen Euklidischen Ring.
- Die Menge $\mathbb{Z}[x]$ der Polynome über \mathbb{Z} bildet keinen Euklidischen Ring.

aber beinahe:

Es gilt: $\forall p[x], q[x] \in \mathbb{Z}[x] \exists a \in \mathbb{Z}, s[x], r[x] \in \mathbb{Z}[x]: a \cdot p[x] = s[x] \cdot q[x] + r[x]$ und $\deg(r) < \deg(q)$

Computer Algebra 6

Division von Polynomen p und q

Verallgemeinerung von \mathbb{Z} auf beliebige Euklidische Ringe:

- Schulalgorithmus zur schriftlichen Division mit Rest
- Euklidischer Algorithmus zur Bestimmung des ggT
- Erweiterter Euklidischer Algorithmus zur Bestimmung von ggT und Bezout-Koeffizienten s und t : $\text{ggT}(p,q) = s \cdot p + t \cdot q$

Folgerung für Polynome:

- Schriftliche Polynomdivision Laufzeit: $O(n^2)$
- Euklidischer Algorithmus zur Bestimmung des größten gemeinsamen Teilerpolynoms Laufzeit: $O(n^2)$
- Erweiterter Euklidischer Algorithmus zur Bestimmung der Bezout-Polynome $s[x]$ und $t[x]$ für Polynome: $\text{ggT}(p[x],q[x]) = s[x] \cdot p[x] + t[x] \cdot q[x]$

Anm.: Das Teilerpolynom ist nur normiert eindeutig. Achtung: expression swell !
In \mathbb{Z} muss zwischendurch mit den Leitkoeffizienten multipliziert werden.

Computer Algebra 6

Faktorisierung eines Polynoms $p[x] \in \mathbb{Q}[x]$ nach Kronecker

Laufzeit: $O(\exp(n))$

Satz 1:

Wenn $p[x] = s[x] \cdot q[x]$ für $p[x], q[x], s[x] \in \mathbb{Q}[x]$,
dann existieren $a, b, c \in \mathbb{Z}$ und Polynome $p^*[x], q^*[x], s^*[x] \in \mathbb{Z}[x]$
mit $p^*[x] = a \cdot p[x]$; $q^*[x] = b \cdot p[x]$; $s^*[x] = c \cdot s[x]$

Folgerung:

Weil die Teilerpolynome ohnehin nur bis auf Normierung
eindeutig sind, lösen wir das Problem gleich in $\mathbb{Z}[x]$

Satz 2:

Die Koeffizienten eines Polynoms vom Grad n sind durch
die Angabe von $n+1$ Funktionswerten eindeutig bestimmt.

1. Erweitere $p[x]$ zu einem ganzzahligen Polynom. Laufzeit: $O(n)$
2. Berechne die ganzzahligen Funktionswerte an $n/2 + 1$ Stützstellen. $O(n^2)$
3. Betrachte die ganzzahligen Teiler der $n/2 + 1$ Funktionswerte
und bilde alle Kombinationen von $(n/2 + 1)$ -Tupeln daraus. $O(\exp(n))$ mal:
4. Ermittle für jede Kombination das Kandidatenpolynom durch Interpolation. $O(n^2)$
5. Teste jeden Kandidaten durch Polynomdivision in $\mathbb{Z}[x]$ $O(n^2)$

Computer Algebra 6

Quadratfreie Faktorisierung mit Ableitungen

Laufzeit: $O(m^3)$

Die Quadratfreie Faktorisierung von einem Polynom $a(x)$ ist gegeben durch:

$$a(x) = \prod_{k=1}^m a_k^k(x)$$

wobei m der Grad von $a(x)$ ist und $a_k(x)$ nur in irreduzible Polynome zerlegt werden kann, die den Grad 1 haben.

Zudem muss gelten: $\text{ggT}(a_k(x), a_j(x)) = 1 \mid \forall k \neq j$.

Satz: $q[x]$ ist mehrfacher Teiler von $p[x] \Leftrightarrow q[x]$ teilt $p[x]$ und $p'[x]$ (Ableitung nach x)

1. Setze i auf 1 zur Bestimmung der einfachen Teiler.
2. Bestimme $g[x] := \text{ggT}(p[x], p'[x])$
3. Berechne $q[x] := p[x] \text{ div } g[x]$ $q[x]$ ist quadratfrei
4. Berechne $a_i[x] := q[x] \text{ div } \text{ggT}(q[x], g[x])$ $a_i[x]$ besteht aus den Faktoren, die genau i mal vorkommen.
5. Erhöhe i um 1 zur Bestimmung der $i+1$ -fachen Teiler.
6. Setze $p[x] := g[x]$ und fahre fort bei Schritt 2.

Computer Algebra 6

Rationale Funktionen $K(x)$ über einem Körper K

Definition:

$K(x)$ ist die Menge aller rationalen **Funktionen der Form** $p[x] / q[x]$, wobei $p[x], q[x] \in K[x]$ für einen Körper K .

Satz: $K(x)$ ist selbst ein Körper.

Rechenoperationen analog zu Brüchen:

- Addition / Subtraktion durch Erweitern und Addition/Subtraktion des Zählers
- Multiplikation / Division durch Multiplikation der Zähler bzw. Nenner

Computer Algebra 6

Rationale Funktionen $K(x)$ über einem Körper K

Definition:

$K(x)$ ist die Menge aller rationalen **Funktionen der Form** $p[x] / q[x]$, wobei $p[x], q[x] \in K[x]$ für einen Körper K .

Satz: $K(x)$ ist selbst ein Körper.

Normierte Darstellung:

$r(x) = p[x] / q[x]$ ist in normierter Darstellung, wenn $\text{ggT}(p[x], q[x]) = 1$

Errechnung der normierten Darstellung einer rationalen Funktion:

- Bestimmung von $\text{ggT}(p[x], q[x])$
- Kürzen: Polynomdivision von $p[x]$ und $q[x]$ durch $\text{ggT}(p[x], q[x])$

Alle rationalen Operationen in $O(n^2)$ möglich (Einheitskostenmaß!)